

# The concrete theory of numbers : Problem of simplicity of Fermat number-twins

Boris V. Tarasov\*

---

February 1, 2008

## Abstract

The problem of simplicity of Fermat number-twins  $f_n^\pm = 2^{2^n} \pm 3$  is studied. The question for what  $n$  numbers  $f_n^\pm$  are composite is investigated. The factor-identities for numbers of a kind  $x^2 \pm k$  are found.

## 1 Introduction

In present work we consider Fermat numbers

$$f_n = 2^{2^n} + 1, \quad (1)$$

where  $n \geq 0$  is integer.

Fermat number-twins we will define as :

$$\begin{aligned} f_n^- &= f_n - 4 = 2^{2^n} - 3, \\ f_n^+ &= f_n + 2 = 2^{2^n} + 3, \end{aligned} \quad (2)$$

where  $n \geq 0$  is integer( for  $f_n^-$  is considered  $n \geq 1$  ).

Pierre de Fermat in 1640 in the letter to Mersenne [1] suggested a hypothesis, that all numbers (1) are prime, which has been denied by Leonhard Euler [2] in 1732, Euler has found decomposition

$$f_5 = 641 \cdot 6700417.$$

Eisenstein (1844) assumed, that there exists infinite number of prime Fermat numbers. There was a well-known problem of Fermat prime [3, 7, Eisenstein].

**Problem 1 (Fermat prime).** *Whether there are infinitely many Fermat prime ?*

---

\*Tarasov Boris V. The concrete theory of numbers: Problem of simplicity of Fermat number-twins. MSC 11A51. ©2007 Tarasov B. V., independent researcher of Unknown.

There was also other not less known problem :

**Problem 2 (Fermat composite numbers).** *Whether there are infinitely many Fermat composite numbers ?*

Problems 1 and 2 are actual even for today. Therefore the researches, throwing light on numbers, located closely to Fermat numbers are extremely useful. Probably, the similar information will reveal a secret of the Fermat numbers in the future.

Five Fermat prime numbers [3, 5, 7, 8, Fermat prime] are known  $f_0 = 3$ ,  $f_1 = 5$ ,  $f_2 = 17$ ,  $f_3 = 257$ ,  $f_4 = 65537$ . The author knows only five Fermat prime number-twins( see [9] ) :

$$f_2^- = 13, f_0^+ = 5, f_1^+ = 7, f_2^+ = 19, f_4^+ = 65539.$$

## 2 Prime divisors of Fermat number-twins

Let's bring the simple statements concerning Fermat number-twins.

**Theorem 1.** *The following congruences are fair :*

(1) *If  $n$  is an even number, then*

$$f_n^- \equiv 0(\text{mod } 13). \quad (3)$$

(2) *If  $n = 4k + 3$ , where  $k \geq 0$ , then*

$$f_n^- \equiv 0(\text{mod } 11). \quad (4)$$

*Proof.* 1) Let  $n = 2$ , then  $f_2^- = 2^4 - 3 = 13$ . Let's assume, that congruence (3) is proved for all even numbers  $n$ , where  $n \leq k$ ,  $k$  is even number. Let's consider expression

$$\begin{aligned} f_{k+2}^- - f_k^- &= 2^{2^{k+2}} - 2^{2^k} = (2^{2^k})^4 - 2^{2^k} = 2^{2^k} \{ (2^{2^k})^3 - 1 \} = \\ &= 2^{2^k} (2^{2^k} - 1) \{ (2^{2^k})^2 + 2^{2^k} + 1 \}. \text{ As } 2^{2^k} \equiv 3(\text{mod } 13), \text{ that} \\ (2^{2^k})^2 + 2^{2^k} + 1 &\equiv 3^2 + 3 + 1 = 13 \equiv 0(\text{mod } 13). \text{ We have proved, that} \\ f_{k+2}^- &\equiv 0(\text{mod } 13). \end{aligned}$$

2) If  $k = 0$ , then  $n = 3$ ,  $f_3^- = 2^{2^3} - 3 = 2^8 - 3 = 11 \cdot 23$ .

Let's consider expression  $f_{4k+3}^- - f_3^- = 2^{8 \cdot 2^{4k}} - 2^8 =$   
 $= 2^8 \{ (2^8)^{2^{4k}-1} - 1 \}$ . Further, as  $2^5 \equiv -1(\text{mod } 11)$ ,  
 $2^{15} \equiv -1(\text{mod } 11)$  and  $2^{4k} - 1 \equiv 0(\text{mod } 15)$ , that  
 $(2^8)^{2^{4k}-1} - 1 \equiv 0(\text{mod } 11)$ . □

**Theorem 2.** *If  $n$  is an odd number, then*

$$f_n^+ \equiv 0(\text{mod } 7). \quad (5)$$

*Proof.*  $f_1^+ = 7$ . Let's assume, that congruence (5) is proved for all odd numbers  $n$ , where  $n \leq k$ ,  $k$  is odd number. Let's consider expression

$$f_{k+2}^+ - f_k^+ = 2^{2^{k+2}} - 2^{2^k} = (2^{2^k})^4 - 2^{2^k} = 2^{2^k} \{ (2^{2^k})^3 - 1 \} =$$

$= 2^{2^k}(2^{2^k} - 1)\{(2^{2^k})^2 + 2^{2^k} + 1\}$ . As  $2^{2^k} \equiv -3 \pmod{7}$ , that  $(2^{2^k})^2 + 2^{2^k} + 1 \equiv 3^2 - 3 + 1 = 7 \equiv 0 \pmod{7}$ . We have proved, that  $f_{k+2}^- \equiv 0 \pmod{7}$ .  $\square$

**Lemma 1.** *The following congruences are fair :*

$$\begin{aligned} 2^{18k+2} + 3 &\equiv 0 \pmod{7}, \\ 2^{18k+4} + 3 &\equiv 0 \pmod{19}, \\ 2^{18k+8} + 3 &\equiv 0 \pmod{7}, \\ 2^{18k+14} + 3 &\equiv 0 \pmod{7}, \end{aligned} \tag{6}$$

where  $k \geq 0$  is integer.

*Proof.* Validity of congruences (6) follows obviously from the equality  $2^{18} - 1 = 3^3 \cdot 7 \cdot 19 \cdot 73$ .  $\square$

**Lemma 2.** *The following statements are fair, where  $t \geq 0$  is integer :*

- (1) If  $2^t - 1 \equiv 0 \pmod{9}$ , then  $t = 6k$ .
- (2) If  $2^t + 1 \equiv 0 \pmod{9}$ , then  $t = 6k + 3$ .

*Proof.* 1) Let  $2^t - 1 \equiv 0 \pmod{9}$  and  $t = 6k + r$ , where  $0 \leq r < 6$ . As  $2^6 - 1 \equiv 0 \pmod{9}$ , that  $2^t - 1 \equiv 2^r - 1 \equiv 0 \pmod{9}$ . As  $2^0 - 1 \equiv 0 \pmod{9}$ , but  $2^1 - 1 = 1 \not\equiv 0 \pmod{9}$ ,  $2^2 - 1 = 3 \not\equiv 0 \pmod{9}$ ,  $2^3 - 1 = 7 \not\equiv 0 \pmod{9}$ ,  $2^4 - 1 = 15 \not\equiv 0 \pmod{9}$ ,  $2^5 - 1 = 31 \not\equiv 0 \pmod{9}$ , that  $r = 0$ . We have proved, that  $t = 6k$ .

2) Let  $2^t + 1 \equiv 0 \pmod{9}$  and  $t = 6k + r$ , where  $0 \leq r < 6$ . Then  $2^t + 1 \equiv 2^r + 1 \equiv 0 \pmod{9}$ . As  $2^0 + 1 = 2 \not\equiv 0 \pmod{9}$ ,  $2^1 + 1 = 3 \not\equiv 0 \pmod{9}$ ,  $2^2 + 1 = 5 \not\equiv 0 \pmod{9}$ ,  $2^4 + 1 = 17 \not\equiv 0 \pmod{9}$ ,  $2^5 + 1 = 33 \not\equiv 0 \pmod{9}$ , but  $2^3 + 1 = 9 \equiv 0 \pmod{9}$ , that  $r = 3$ . We have proved, that  $t = 6k + 3$ .  $\square$

**Theorem 3.** *The following statements are fair :*

- (1) Prime numbers  $f_n^-$ ,  $n > 2$  are possible only for  $n = 4k + 1$ , where  $k \geq 1$ .
- (2) Prime numbers  $f_n^+$ ,  $n > 4$  are possible only for  $n = 6k$  or  $n = 6k + 4$ , where  $k \geq 1$ .

*Proof.* The statement (1) is the corollary of the theorem 1. Let's prove the statement (2). Let's assume, that number  $f_n^+$  is prime. Then it follows from a lemma 1, that if  $2^n = 18m + r$ , where  $0 \leq r < 18$ ,  $r$  is an even number, then  $r = 10$  or  $r = 16$ . If  $2^n = 18m + 10$ , then  $2^n - 1 \equiv 0 \pmod{9}$ . Then it follows from a lemma 2, that  $n = 6k$ . If  $2^n = 18m + 16$ , then  $2^n + 2 \equiv 0 \pmod{9}$  or  $2^{n-1} + 1 \equiv 0 \pmod{9}$ . Then it follows from a lemma 2, that  $n - 1 = 6k + 3$  or  $n = 6k + 4$ .  $\square$

It is checked up, that for  $n > 2$ ,  $n = 4k + 1$ , where  $0 < k \leq 4$ , i.e. for  $n = 5, 9, 13, 17$  numbers  $f_n^-$  are composite. It is checked up, that for  $n > 4$ ,

$n = 6k$  and  $n > 4$ ,  $n = 6k + 4$ , where  $0 < k \leq 2$ , i.e. for  $n = 6, 10, 12, 16$  numbers  $f_n^+$  are composite.

**Remark** (MMonline). *M. Alekseyev [10] at the forum MMonline "Mathematics" furnishes without the proof the statement :*  
*If  $n = 12k + 10$ , then  $f_n^+ \equiv 0 \pmod{79}$ .*

Thus,  $f_n^+$  are composite and for  $n = 6k + 4$ , where  $k \geq 1$  is an odd number.

**Theorem 4.** *Numbers  $f_n^-$  and  $f_n^+$  are simultaneously composite for all  $n$  of kind :*

$$\begin{aligned} n &= 12k + 2, & (1^\circ) \\ n &= 12k + 3, & (2^\circ) \\ n &= 12k + 7, & (3^\circ) \\ n &= 12k + 8, & (4^\circ) \\ n &= 12k + 11, & (5^\circ) \end{aligned} \tag{7}$$

where  $k \geq 1$  is integer.

*Proof.* Validity of the theorem 4 follows obviously from statements of the theorem 3.  $\square$

### 3 The factor-identities for numbers of a kind $X^2 \pm k$

For the beginning, let's bring two known identities.

#### 3.1 The first factor-identity

$$1 + (L^2 + L + 1)^2 = (L^2 + 1) \cdot (L^2 + 2L + 2), \tag{8}$$

where  $L \geq 1$  is integer.

#### 3.2 The second factor-identity

$$1 + (2L^2)^2 = (2L^2 - 2L + 1) \cdot (2L^2 + 2L + 1), \tag{9}$$

where  $L > 1$  is integer.

### 3.3 The new factor-identity

If

$$\begin{aligned} A &= a + amnk + n^2/4 \cdot (am^2 + n^2)k^2, \\ B &= 1 - mnk + m^2/4 \cdot (am^2 + n^2)k^2, \\ X &= 1/2(am^2 - n^2)k + mn/4 \cdot (am^2 + n^2)k^2, \end{aligned} \quad (10)$$

where  $m, n, k, a$  are integer, then equality takes place

$$a + X^2 = A \cdot B. \quad (11)$$

The author does not know the factor-identity of type  $1 + X^2 = AB$ , left part of which contains an infinite subset of Fermat numbers. Existence of such factor-identity positively solves the [problem 2](#), that there exists the infinite number of composite Fermat numbers !

## 4 The conclusion

If number of prime Fermat  $f_n$  is finite, that, starting from a number  $k_0 > 1$ , for all numbers  $n$  from (7), where  $k > k_0$ , we receive an infinite sequence of compound numbers with 9 numbers in a part, namely

$$f_n - 5, f_n - 4, f_n - 3, f_n - 2, f_n - 1, f_n, f_n + 1, f_n + 2, f_n + 3. \quad (12)$$

Such gaps from composite numbers are too regular. The author supports the [assumption](#) of the Eisenstein(1844), that [there exists the infinite number of prime Fermat numbers](#) !

The author offers a problem as a unresolved task :

**Problem 3** ([Prime Fermat number-twins](#)). *Whether there are prime Fermat number-twins  $f_n^\pm$  for  $n > 4$  ?*

As it was already noted, numbers  $f_2^- = 13$ ,  $f_0^+ = 5$ ,  $f_1^+ = 7$ ,  $f_2^+ = 19$ ,  $f_4^+ = 65539$  are prime. It is checked up by the author, that for  $n \leq 17$  there is no other prime Fermat number-twins.

## References

- [1] Pierre de Fermat. *Letter to Marin Mersenne*(25 December 1640), *CEuvres de Fermat*, volume 2, 212-217.
- [2] Euler, L. "Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus." *Acad. Sci. Petropol.* 6, 103-107, ad annos 1732-33(1738). In *Leonhardi Euleri Opera Omnia*, Ser. I, Vol. II. Leipzig: Teubner, pp. 1-5, 1915.
- [3] Arnold I.V. *Teoriya chisel*. - M.: Uchpedgiz, 1939.
- [4] Vinogradov I. M. *Osnovy teorii chisel*. - M.: Nauka, 1981.
- [5] Ronald L. Graham, Donald E. Knuth, Oren Patashnik. *Concrete Mathematics : A Foundation for Computer Science*, 2nd edition (Reading, Massachusetts: Addison-Wesley), 1994.
- [6] Ribenboim, P. "Fermat Numbers" and "Numbers  $k \times 2^n \pm 1$ ." §2.6 and 5.7 in *The New Book of Prime Number Records*. New York: Springer-Verlag, pp. 83-90 and 355-360, 1996.
- [7] Weisstein, Eric W. "Fermat Number". From *MathWorld*—A Wolfram Web Resource. —<http://mathworld.wolfram.com/FermatNumber.html/>. ©1999—2007 Wolfram Research, Inc.
- [8] *Distributed Search for Fermat Number Divisors*. —<http://www.fermatsearch.org/>.
- [9] Sloane, N. J. A. *Sequences A057732 and A050414* in "The On-Line Encyclopedia of Integer Sequences."
- [10] Boris Tarasov. *Interesnaya zadachka na sravnimost' celix chisel !* —<http://www.mmonline.ru/forum/read.php?f=1&i=6616&t=6616>

---

Institute of Thermophysics, Siberian Branch of RAS  
 Lavrentyev Ave., 1, Novosibirsk, 630090, Russia  
 E-mail: tarasov@itp.nsc.ru

---

Boris Vladimirovich Tarasov,  
 Independent researcher of Unknown,  
 E-mail: tarasov-b@mail.ru

---